BROADCAST SERVICE ACCESS CONTROL

Publication number: JP2002518935 (T)
Publication date: 2002-06-25
Inventor(s):
Applicant(s):
Classification:
- international: ***H04H60/23; H04H60/91; H04L29/06; H04L9/08; H04W12/02; H04W4/06;*** *H04W12/04; H04W12/06;* **H04L29/06; H04L9/08; H04W12/00; H04W4/06;** (IPC1-7): H04L9/08; H04Q7/38
- European: H04H60/23; H04H60/91; H04L29/06C8; H04L29/06S4B; H04L29/06S6; H04L9/08; H04Q7/22S; H04Q7/38C2D; H04W12/02; H04W4/06
Application number: JP20000555388T 19990528
Priority number(s): WO1999SE00929 19990528; US19980089280P 19980615; US19980092592P 19980710; US19980132232 19980811

Also published as:
WO9966670 (A1)
US6510515 (B1)
NZ508561 (A)
KR20060076327 (A)
KR100695862 (B1)
more >>

Abstract not available for JP 2002518935 (T)
Abstract of corresponding document: **WO 9966670 (A1)**

Techniques and systems for controlling access to information broadcast over point-to-multipoint resources in radiocommunication systems are described. These techniques can be used to provide controllable access to broadcast information services, e.g., security quote services, sports information services, etc., which broadcast services can be provided in conjuction with more conventional cellular radiocommunication services, e.g., voice calls. Exemplary embodiments of the present invention enable subscribing users' equipment to output broadcast information using, for example, either a status variable within the remote equipment or encryption for which subscribing devices have a corresponding decryption key.

(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－518935
（P2002－518935A）
(43)公表日　平成14年６月25日(2002.6.25)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ	５Ｊ１０４
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７

審査請求　未請求　予備審査請求　有　（全 50 頁）

(21)出願番号　特願2000－555388(P2000－555388)
(86)(22)出願日　平成11年５月28日(1999.5.28)
(85)翻訳文提出日　平成12年12月14日(2000.12.14)
(86)国際出願番号　ＰＣＴ／ＳＥ９９／００９２９
(87)国際公開番号　ＷＯ９９／６６６７０
(87)国際公開日　平成11年12月23日(1999.12.23)
(31)優先権主張番号　６０／０８９，２８０
(32)優先日　平成10年６月15日(1998.6.15)
(33)優先権主張国　米国（ＵＳ）
(31)優先権主張番号　６０／０９２，５９２
(32)優先日　平成10年７月10日(1998.7.10)
(33)優先権主張国　米国（ＵＳ）

(71)出願人　テレフオンアクチーボラゲット　エル　エム　エリクソン（パブル）
スウェーデン国エス　－　126　25　ストックホルム
(72)発明者　ライス，　クリスター，　アレックス
アメリカ合衆国　ノース　カロライナ州　27713，　ダーハム，　パーク　リッジ　アヴェニュー　805－エー５
(74)代理人　弁理士　大塚　康徳　（外１名）

Ｆターム(参考)　5J104 AA01 AA16 BA03 EA01 EA04 EA15 EA17 NA02 NA05 PA01
5K067 AA30 HH36

最終頁に続く

(54)【発明の名称】　報知サービスに対するアクセス制御方法及びシステム

(57)【要約】
無線通信システムにおけるポイントツーマルチポイントリソースを介して報知される情報へのアクセスを制御する方法及びシステムが説明される。これら方法は例えば証券相場サービス、スポーツ情報サービス等の報知情報サービスであって、より一般的なセルラ式無線通信サービス、例えば音声セルとともに提供可能な報知情報サービスに対するコントローラブルなアクセスを提供するために使用可能である。本発明の実施例は購読ユーザの装置に、例えばリモート装置内部の状態変数又は、購読装置が対応する復号鍵を有する暗号化のいずれかを用いて報知情報を出力することを可能とする。

【特許請求の範囲】

【請求項１】　無線通信システムにおける報知情報サービスに対するアクセスを制御する方法であって、

前記報知情報サービスに関連する情報を暗号化するステップと、

前記システムによって、前記暗号化された、複数のリモートユニットによって利用可能な情報をエア・インタフェースを介して報知するステップと、

前記暗号化された情報を、前記複数のリモート局のうちの購読中の１つへアドレス指定されたメッセージの一部として復号するために利用可能なサービス鍵を前記システムによって伝送するステップ、及び、

前記サービス鍵を周期的に変化させるステップとを有することを特徴とする方法。

【請求項２】　前記サービス鍵を前記システムによる伝送前に暗号化するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項３】　前記サービス鍵を暗号化するステップが、

前記サービス鍵をＡ鍵手法を用いて暗号化するステップをさらに有することを特徴とする請求項２記載の方法。

【請求項４】　前記サービス鍵の受信を、前記複数のリモート局のうちの購読中の１つによってアクノリッジするステップをさらに有することを特徴とする請求項１記載の方法。

【請求項５】　前記サービス鍵を伝送するステップが、

前記サービス鍵の伝送にＯＡＴＳ(Over-the-air Activation TeleService)を用いるステップをさらに含むことを特徴とする請求項４記載の方法。

【請求項６】　前記サービス鍵を伝送するステップが、

前記サービス鍵を報知チャネルで伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項７】　前記サービス鍵を伝送するステップが、

前記サービス鍵をポイントツーポイントチャネルで伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項８】　さらに、

前記変更されたサービス鍵を用いて前記情報を暗号化する前に、所定時間前記変更されたサービス鍵を前記複数のリモート局のうち現在購読中のリモート局に対して伝送するステップを有することを特徴とする請求項１記載の方法。

【請求項９】　前記情報を暗号化するステップが、前記情報を所定の変数を用いてスクランブルするステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１０】　前記サービス鍵を伝送するステップが、

前記サービス鍵とともに、前記サービス鍵が前記情報の復号化に利用可能な有効期間を伝送することを特徴とする請求項１記載の方法。

【請求項１１】　前記サービス鍵を伝送するステップが、

前記サービス鍵とともに、リモート装置が前記サービス鍵が有効であるかどうかを判断するのに利用可能なキーインデックスを伝送する方法。

【請求項１２】　前記サービス鍵を伝送するステップが、

個人識別番号（ＰＩＮ）及びサービス識別番号（ＳＩＮ）の１つを前記サービス鍵として供給するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１３】　さらに、

前記複数のリモート局のうちの前記現在購読中の１つにおいて、前記変更されたサービス鍵及び前記サービス鍵を保存するステップ及び、

前記システムによって１回に報知された前記情報の復号に前記変更されたサービス鍵を用いるステップを有することを特徴とする請求項８記載の方法。

【請求項１４】　前記サービス鍵を伝送するステップが、

前記サービス鍵を周期的な間隔で繰り返し伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１５】　無線通信システムにおける報知情報サービスに対するアクセスを制御する方法であって、

前記報知情報サービスに関連する情報であって、複数のリモートユニットが利用可能な情報を、前記システムによってエア・インタフェースを介して伝送するステップと、

有効化信号を、前記複数のリモート局のうち購読中のリモート局宛のメッセージの一部として、前記システムによって伝送するステップ、及び、

前記複数のリモートユニットの１つが自分に宛てられた有効化信号を受信した場合、前記複数のリモートユニットの１つにおいて前記情報を出力するステップとを有することを特徴とする方法。

【請求項１６】　前記複数のリモート局のうち購読中のリモート局によって、前記有効化信号の受信をアクノリッジするステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１７】　前記有効化信号を伝送する前記ステップが、

前記有効化信号を報知チャネルで伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１８】　前記有効化信号を伝送する前記ステップが、

前記有効化信号をポイントツーポイントチャネルで伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１９】　前記有効化信号を伝送する前記ステップが、

前記有効化信号を周期的な感覚で繰り返し再伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項２０】　少なくとも１つの報知リソースにおいて報知情報サービスに関連する報知情報を受信するとともに、前記報知情報サービスに関連する有効化及び無効化メッセージを受信する受信機と、

前記有効化及び無効化メッセージの受信に基づいて値が変化する、有効化／無効化状態変数を保持するメモリ装置、及び、

前記有効化／無効化状態変数が有効化の値を有する場合のみ前記報知情報を出力する出力装置とを有することを特徴とする移動局。

【請求項２１】　前記購読中のリモート局が前記暗号化情報へのアクセスを得るための料金を負うことを特徴とする請求項１記載の方法。

【請求項２２】　前記料金が銀行口座又は前払い口座から控除されることを特徴とする請求項２１記載の方法。

【請求項２３】　前記料金がクレジット口座につけられることを特徴とする

請求項２１記載の方法。

【請求項２４】　少なくとも１つの報知リソースにおいて報知情報サービスに関連する暗号化された報知情報を受信するとともに、前記暗号化された情報を復号するために利用可能なサービス鍵を受信する受信機と、

前記サービス鍵を保持するメモリ装置、及び、

前記暗号化情報が前記サービス鍵によって復号され次第前記報知情報を出力する出力装置とを有することを特徴とする移動局。

【請求項２５】　前記サービス鍵が前記報知情報サービスによって伝送される前に暗号化されていることを特徴とする請求項２４記載の移動局。

【請求項２６】　前記サービス鍵がＡ鍵手法に従って暗号化されていることを特徴とする請求項２５記載の移動局。

【請求項２７】　前記サービス鍵が予め定められた期間有効であることを特徴とする請求項２４記載の移動局。

【請求項２８】　前記受信機が予め定められた期間の満了前に、次のサービス鍵を受信することを特徴とする請求項２７記載の移動局。

【請求項２９】　報知情報サービスを当該報知情報サービスの購読者に提供する無線通信システムであって、

前記報知情報を暗号化する暗号化手段と、

前記暗号化された報知情報及び前記暗号化された報知情報の復号に使用可能な鍵を伝送する伝送手段、及び、

前記暗号化された報知情報及び前記伝送された鍵を受信する、少なくとも１つのリモート受信手段とを有し、

さらに前記受信手段が、

前記鍵を前記暗号化された情報の復号に用いるプロセッサ手段と、

前記復号された情報を出力する出力手段とを有することを特徴とする無線通信システム。

【請求項３０】　前記情報が受信されてから予め定められた時間後、前記出力手段によって出力されることを特徴とする請求項２９記載の無線通信システム。

【請求項３１】　前記情報が金融市場動向を含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３２】　前記情報がスポーツのスコアを含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３３】　前記情報がニュースの見出しを含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３４】　無線通信システムにおける報知情報サービスへのアクセスを提供する方法であって、

前記報知情報サービスに関連する情報の部分を暗号化するステップと、

前記システムによって、前記報知情報サービスに関連する情報であって、複数のリモートユニットに利用可能な情報を、エア・インタフェースを介して報知するステップと、

前記システムによって、前記情報の暗号化された部分を復号するのに使用可能なサービス鍵を、前記複数のリモート局のうちの、選択されたリモート局宛てメッセージの一部として伝送するステップ、及び、

前記サービス鍵を周期的に変更するステップとを有することを特徴とする方法。

【請求項３５】　前記鍵が前記リモート局のうち購読中のリモート局に伝送されることを特徴とする請求項３４記載の方法。

【請求項３６】　前記報知情報が前記報知情報サービスのための宣伝メッセージを含み、前記メッセージが前記リモート局のうち、購読中でないリモート局へ送信されることを特徴とする請求項３４記載の方法。

【発明の詳細な説明】
【０００１】
（背景技術）
本発明は一般に無線通信システムにおける情報サービスの提供に関し、特に、既存の無線通信サービス及びシステムとともに供給される放送情報サービスへのアクセス制御技術に関する。
【０００２】
商用無線通信の成長は過去１５年間に渡って劇的であった。特にポケットベル及びセルラ式電話は多くの都市環境において比較的一般的な設備として特出している。これら２つの異なるタイプの通信装置及びそれをサポートするシステムは異なる根本的な目的、すなわちポケットベルは伝統的に一方向で限られた情報を一人かそれより多いユーザに提供する、セルラ式電話は伝統的に双方向音声通信サービスを提供するという目的から発展してきた。
【０００３】
時間が流れ、技術が進歩するに連れて、これら２つの異なるタイプの無線通信装置を分ける伝統的、機能的境界は曖昧になってきた。ポケットベルはセルラ式電話によって伝統的に提供されていたいくつかの機能を獲得し、また逆の現象も生じている。例えば、ポケットベルから呼び出しシステムへ、呼び出しシステムによって他の加入者へ転送されうるメッセージの送信を許可する双方向ポケットベルが開発されている。同様に、セルラ式電話は電話機のディスプレイに表示されうる（例えば英数字(alphanumeric character)１６０文字程度の）ショートテキストメッセージの送信及び受信機能を獲得した。この無線通信装置における革命は新たな情報サービスのホスト開発及びマーケティングをもたらしてきた。
【０００４】
従来のセルラシステムへのアプリケーションのための報知情報サービスが開発されたため、ネットワークオペレータ及び／又はサービスプロバイダにこれら新しいサービスへのアクセスを制御可能とさせる技術を与えることは望ましいと出願人は予想する。歴史的に、無線サービスに対するアクセス制御／セキュリティは次の４つの一般的な無線サービスの中で変化する。（１）ポイントツーポイン

トサービス、例えば２つのリモート端末間における音声通信、（２）グループ発呼、すなわち２つより多くのリモート端末間における音声通信、（３）ノンエンドユーザによるポイントツーマルチポイントサービス、例えばシステム制御報知情報及び、（４）エンドユーザによるポイントツーマルチポイントサービス、例えば証券相場サービス、スポーツスコアサービス等。

【０００５】

今日におけるポイントツーポイントサービスの大部分は固定電話網もしくは他の移動局ユーザへなされる音声通話で構成される。不正利用の削減や盗聴を制限するため、認証及び暗号化はまもなくサービスを開始する個人通信向けの衛星システムを含むすべてのディジタルセルラシステムにおいてサポートされる。各移動電話（またはＧＳＭ規格に従って動作する移動電話におけるＳＩＭカード）は秘密鍵を有する。この鍵は認証及び暗号化の根元(root)であり、各ユーザの秘密鍵はユニークである。電気通信工業会(TIA: Telecommunications Industry Association)によって公開されるセキュリティ仕様においてＡキー(A-key)と呼ばれるこの鍵は、キーボードによってユーザが入力可能か、ＴＩＡ仕様に説明される無線アクティベーションテレサービス(Over-the-Air Activation Teleservice（OATS))手順において送信もしくは生成されることができる。ＧＳＭにおいて、鍵は"スマートカード"（ＳＩＭカード）に存在し、変更することはできない。認証はシステムにユーザ（より具体的には電話機もしくはＳＩＭカード）の確認を実現させる。伝送の暗号化はシステムの違法な利用、例えば不正な情報を移動局へ送信することをより制限する。基地局が必ず自らの正当性をも確認しなければならない双方向認証は、移動局へダミーデータを送信している不正な基地局をもつリスクを削減する。

【０００６】

ポイントツーポイント通信サービスに類似したサービスはグループコールである。グループコールが個々のトラフィックチャネルに割り当てられた各メンバによって設定された場合、２個人間の、より"普通の"通話に関しては、個々のＡキーに基づく認証及び暗号化が利用でき、さらなる保護手順を必要とする通常の音声通話とグループコールとの間に違いはない。グループに割り当てられた、特

にダウンリンクにおいて利用可能な共通チャネルがある場合、全ユーザはこのチャネルを受信(listen)できねばならない。従って、この場合のダウンリンクの暗号化は特定のユーザのＡキーに基づいて行うことはできない。暗号化にはグループに共通な暗号鍵（Ｇキー）を用いなければならない。各ユーザは依然として個人ベースで、例えば標準のＡキーを用いて認証をうけることが可能である。しかしながら、暗号鍵は誰かのＡキーのルートキーであってはならない。Ｇキーはキーパッドを用いて、あるいは通常のＡキーに基づく暗号化の保護の元で移動局に送信されることによって移動局に入力される。

【０００７】

例えばセルラシステムにおいて報知制御チャネル（ＢＣＣＨ）で提供される情報のようなノンエンドユーザポイントツーマルチポイントサービスでは、現在の無線システムに適切な保護機構は存在しない。このタイプのリソースに存在する制御情報を移動局が高速かつ容易に見つけて読むことが可能なようにシステム設計者は欲するため、これは問題である。このサービスタイプについて、非購読ユーザがＢＣＣＨ上に報知される制御情報を読むことを妨害するための誘因はほとんどもしくは全くない。しかし、データの正当性を確認する技術は提供される。従って、ポイントツーマルチポイント制御チャネルへのアクセスを妨害するための暗号化は必要でないか提供されていない。

【０００８】

例えば上述した、本明細書に組み入れられる２件の特許出願に開示される証券相場やヘッドラインサービスのようなエンドユーザポイントツーマルチポイントサービスは、サービスオペレータ（セルラオペレータと同一である必要はない）におけるノンエンドユーザポイントツーマルチポイントサービスと異なり、エアインタフェースを介して購読者に報知される情報を非購読の個人に読ませたくはない。例えば、報知チャネルで証券相場が提供されている場合、毎月の購読料を支払っていないユーザは情報へのアクセスが不可能であるべきである。報知制御情報については、購読エンドユーザへ報知されるデータサービスのためのデータ正当性保護もまた望まれるところであろう。

【０００９】

従って、適切な情報正当性及びアクセス制御レベルを提供する、報知情報サービスへのアクセスを制御する方法及びシステムの提供は好ましいことであると思われる。ここで、方法やシステムの関与は操作の容易性（例えば、購読者のアクティベーション／デアクティベーションの容易性）に対してバランスが取られる。

【００１０】

（発明の概要）

本発明の典型的な実施例は無線通信システムを介して提供される報知情報サービスについてのアクセス制御をサポートする技術を提供する。本発明によるサービスアクセス制御技術は多くの目的の達成を試みる。具体的には、正当なユーザのみがサービスを受信可能であり、特定のユーザに対して簡単かつ素早くサービスを提供可能であり、特定のユーザに対して簡単かつ素早くサービスの提供を取り止めることが可能であり、報知チャネルまたはサブチャネルに不正なメッセージを挿入することが困難であり、サービスにアクセスできないので請求には応じられないというユーザのクレームに対しオペレータが確認可能である。エンドユーザの装置、例えば移動局は単純なポケットベルのような受信専用の装置であっても、移動電話機のような送受信装置であってもよい。

【００１１】

本発明の純粋な実例であり、典型的な実施例によれば、報知情報サービスは報知ショートメッセージサービス（ＳＭＳ）機能を有する、ＩＳ－１３６規格準拠のシステムにおいて提供される証券相場サービス(security quote service)であってよい。ＩＳＭ－３６において使用予約されている報知制御チャネルの一部を、証券相場サービスの実施に用いられるデータの様々な部分を搬送するための複数の論理サブチャネルにさらに分割することができる。より具体的には、これらの典型的なサブチャネルは証券名チャネル(Security Name channel)、開始値チャネル(Start Value channel)及びデルタチャネル(Delta channel)を含んでよい。

【００１２】

これらのチャネルへのアクセスは異なる技術を用いて提供されてよい。第１の

典型的な実施例によれば、リモート装置のユーザが特定の報知サービスに関連する情報の受信に対する認証を受けているかどうかを通知するステータス変数をリモート装置において維持することができる。リモート装置はこのステータス変数をチェックし、それに従って選択的に情報を出力する。サービスプロバイダはこのステータス変数を更新するために有効／無効信号を周期的に送信することが可能である。

【００１３】

本発明の他の典型的な実施例によれば、報知チャネルを伝送される情報は暗号化されてよい。そして、購読者は報知情報の暗号化を解読可能なキーを周期的に受信する。

【００１４】

本発明の上述の目的及び機能は添付した図面と以下の好ましい実施例の説明からさらに明らかになるであろう。

【００１５】

【実施例】

（詳細な説明）

以下の説明はセルラ式無線電話システムに関して書かれているが、出願人の発明はその環境に限定されないということは理解されるであろう。また、以下の説明はＴＤＭＡセルラ式通信システムであるＩＳ－１３６規格準拠という環境において記載されるが、（上述の通り）本発明が例えばＧＳＭやＰＤＣ、さらにＩＳ－９５のようなＣＤＭＡを用いるような他の標準に従って設計された他のディジタル通信アプリケーションにおいても実施可能であることは本発明の当業者には理解されよう。

【００１６】

特に、本発明の典型的な実施例はサービスオペレータによってアクセスが制御されるような報知情報サービスを提供する技術及びシステムを説明する。アクセス制御技術を論じるためのいくつかの文脈を提供するため、まず最初に典型的な報知サービス、すなわちＩＳ－１３６において利用可能な報知リソース、特に報知ＳＭＳチャネル（Ｓ－ＢＣＣＨ）を用いてオペレータによって提供される報知

サービスについて説明する。ＩＳ－１３６システム全体及び報知ＳＭＳチャネルに関するいくつかの詳細は以下において特別に説明されるが、それ以外については本発明を不明瞭にすることを避けるため省略する。しかし、興味のある読者はＩＳ－１３６関連システム全体及び報知ＳＭＳ技術の詳細に関連するさらなる情報のために、Raith等の米国特許第５，６０３，０８１号及び米国特許出願第０８／４８２，７５４号をそれぞれ参照することができる。上述の米国特許及び米国特許出願のいずれも明確に本明細書に参照として組み入れられる。

【００１７】

出願人の発明の典型的な実施例において、基地局から移動局への情報伝送は連続する異なる種類の論理フレームで構成される。図１はＩＳ－１３６による、順方向（forward:基地局から移動局への）方向のＤＣＣＨにおけるフレーム構成および、各ハイパーフレームが好ましくはそれぞれの１次スーパフレーム(primary superframe：ＳＦ）及び２次スーパフレームを含む、２つの連続するハイパーフレーム（ＨＦ）を示している。もちろん、ハイパーフレームは２つ以上のスーパフレームを含んでもよいことは理解されるであろう。

【００１８】

図１には、３つの連続するスーパフレームが示されている。各スーパフレームは以下に説明される論理チャネルＦ－ＢＣＣＨ、Ｅ－ＢＣＣＨ、Ｓ－ＢＣＣＨ及びＳＰＡＣＨとして編成される複数のタイムスロットを有している。ここで、順方向ＤＣＣＨ(forward DCCH)における各スーパフレームはＦ－ＢＣＣＨ情報の完全セット(complete set)、すなわちレイヤ３メッセージのあるセットを必要な数のスロットを用いて含んでおり、かつ各スーパフレームがＦ－ＢＣＣＨスロットから始まることに注意しておくことが好ましい。１つかそれより多いＦ－ＢＣＣＨスロットの後、各スーパフレームの残りのスロットはＥ－ＢＣＣＨ、Ｓ－ＢＣＣＨ及びＳＰＡＣＨ論理チャネルのための１かそれより多い（もしくはゼロの）スロットを含む。

【００１９】

図１並びに特に図２を参照して、ダウンリンク（順方向）ＤＣＣＨの各スーパフレームは好ましくは報知制御チャネルＢＣＣＨ及びショートメッセージサービ

ス／呼び出し／アクセスチャネルＳＰＡＣＨを有する。ＢＣＣＨは高速ＢＣＣＨ（fast BCCH：図１にＦ－ＢＣＣＨとして示される）、拡張ＢＣＣＨ（extended BCCH：Ｅ－ＢＣＣＨ）及びショートメッセージサービスＢＣＣＨ（Ｓ－ＢＣＣＨ）から構成され、そのうちのいくつかは主に一般的なシステム関連情報を基地局から移動局へ搬送するのに用いられる。

【００２０】

Ｆ－ＢＣＣＨ論理チャネルはＤＣＣＨの構成など、時間に制約のあるシステム情報(time-critical system information)、システムへのアクセスに不可欠な他のパラメータ及びＥ－ＢＣＣＨ変更フラグ（本フラグについては上述した、本発明と同一出願人による米国特許出願第０８／４８２，７５４号により詳細な説明がなされており、当該特許出願は本明細書に参照として組み込まれる）を搬送し、Ｆ－ＢＣＣＨ情報の完全セットはすべてのスーパフレームで送信される。Ｅ－ＢＣＣＨ論理チャネルはＦ－ＢＣＣＨで送信される情報よりは時間の制約が少ないシステム情報を搬送する。Ｅ－ＢＣＣＨ情報の完全セット（すなわち、レイヤ３メッセージのあるセット）は、いくつかのスーパフレームに渡ってもよく、スーパフレームの最初のＥ－ＢＣＣＨスロットから開始するように順番をそろえる必要もない。Ｓ－ＢＣＣＨ論理チャネルは、証券情報、宣伝及び移動局購読者のいろいろな組にとって興味のある他の情報など、短い報知メッセージ(short broadcast massage)を搬送する。本発明の典型的な実施例によれば、この論理チャネルは、例えば証券相場サービスのようなポイントツーマルチポイント情報サービスを、Ｓ－ＢＣＣＨチャネルをこの報知情報サービスをサポートする少なくとも３つの論理サブチャネル（証券名チャネル、開始値チャネル及びデルタチャネル。図３参照）に分割することによってサポートするために用いられる。購読ユーザのリモート装置に証券相場情報を出力するのに必要な情報のいろいろな部分(various portion)は、３つのサブチャネルのそれぞれで送信される。これら３つのＳ－ＢＣＣＨサブチャネルが典型的な報知情報サービスを提供するためにどのように用いられるかの詳細について、興味のある読者は、本明細書に組み込まれた上述の特許出願、「無線通信システムを介して送信される情報サービスのためのチャネル化及びエンコード技術(Channelization and Encoding Techniques

for Information Services Transmitted Via Radiocommunication Systems)」を参照されたい。

【００２１】

無線信号を送信して購読ユーザに報知（すなわち、ポイントツーマルチポイント）情報サービスを提供するために適合可能なエアインタフェースの一部について簡単な概要を説明した。もちろん、購読ユーザはまたこれらの伝送を行うためのネットワーク設備及び、この情報を受信するための端末装置が必要である。このような設備は、例えば従来のセルラ設備を含むことができる。例えば、図４は典型的な基地局１１０及び移動局１２０を含む、典型的なセルラ式移動無線電話システムのブロック図である。基地局はＰＳＴＮ（図示せず）に接続されるＭＳＣ１４０へ接続される制御及び処理部１３０を含む。このようなセルラ式無線電話システムの一般的な構成は、Wejke等の米国特許第５，１７５，８６７号、「セルラ通信システムにおける、隣接セルにアシストされるハンドオフ(Neighber-Assisted Handoff in a Cellular Communication System)」及び、１９９２年１０月２７日に出願された米国特許出願第０７／９６７，０２７号、「マルチモード信号処理(Multi-mode Signal Processing)」に開示されるように当該技術分野で知られている。なお、これら２件の特許（特許出願）はいずれも本明細書に参照として組み込まれる。

【００２２】

基地局１１０は複数の音声チャネルを、制御及び処理部１３０に制御される音声チャネル送受信機１５０を通じて取り扱う。また、各基地局は制御チャネル送受信機１６０を有する。制御チャネル送受信機１６０は１つより多い制御チャネルを取り扱い可能であってよい。制御チャネル送受信機１６０は制御及び処理部１３０によって制御される。制御チャネル送受信機１６０は基地局もしくはセルの制御チャネルを通じ、その制御チャネルにロックされた移動局へ制御情報を報知する。同一の無線搬送波周波数を共用する複数のＤＣＣＨ及びＤＴＣを用いるために、送受信機１５０及び１６０が音声及び制御送受信機１７０のように１つの装置として実装されてもよいことは理解されるであろう。

【００２３】

ユーザは、自らが指定(describe)する報知サービスから、従来の移動局１２０を用いて情報を受信する。移動局１２０は制御チャネル上で報知される情報を自らの音声及び制御チャネル送受信機１７０で受信する。そして、処理部１７５が受信した、移動局がロックする候補となるセルの特性を含む制御チャネル情報を評価し、移動局がどのセルにロックすべきかを決定する。

【００２４】

移動局１２０はさらにメモリ１８０及び、ユーザに移動局とのインタラクションを可能とする数字キーパッドのような入力装置１８５とを含む。ＬＣＤ画面のような表示装置１９０はユーザに情報の可視表示を提供する。

【００２５】

本発明は移動局１２０のような従来のリモート端末にも確かに適用可能であるけれども、他のタイプのリモート受信装置に対しても適用可能である。例えば、本発明はリモート装置が受信及び送信能力の両方を持っているようなシステムに適用可能である一方、受信専用の装置、例えば伝統的な呼び出しリモート装置に対しても適用可能である。実際、（１）報知サービスが記述される情報の形式、例えばスポーツスコア、証券相場等はそれ自体リモート装置の電送能力を供給しないこと、（２）送信機能を除去することによりリモート装置のさらなる小型化及び低価格化が可能であることを考慮すると、少なくともいくつかの受信専用のリモート装置を提供することは実体的な動機が存在する。

【００２６】

いずれにしても、リモート装置でサポートされる能力（またはその欠如）に関する知識は、どのタイプの報知サービスアクセス制御（Broadcast Service Access Control：Ｂ－ＳＡＣ）方法を実装するかの決定に有用であろう。例えば、以下の典型的なＢ－ＳＡＣ実施例においては、加入者にアクセス制御情報、例えば暗号鍵の受信を確認させることが好ましいであろうため、送信機能が必要となる。

【００２７】

送信機能に加え、リモート装置のＩ／Ｏインタフェースもまた重要性を異ならせる。例えば、報知証券相場サービスとともに動作することが予期されるリモー

ト装置は精巧なキーボードを必要としない。従って、通常の音声電話機に存在するようなダイヤルパッドはサポートされず、リモート装置は装置に一般的なデータを入力する手段をもたない。替わりに、ユーザがフォルダのスクロール及びフォルダの選択をおこなうための、ただ２，３の「ソフトキー」が必要となる。

【００２８】

従って、報知情報サービスとともに利用可能なリモート装置は、送信（ＴＸ）機能及びローカルデータ入力（ＬＤＥ）機能の存在もしくは欠如に関して以下の表の通り大まかに分類することができる。必要であれば、特定のＢ－ＳＡＣ実施例によってサポートされる（好ましくは特定のＢ－ＳＡＣとともに用いられる）リモート装置のカテゴリに関する好適なコメントがなされている。

【００２９】

【表１】

	装置の機能	
	送信機能	送信機能なし
ＬＤＥ	タイプＡ１	タイプＢ１
ＬＤＥなし	タイプＡ２	タイプＢ２

【００３０】

例えば、ネットワーク及びリモート装置の間の（音声とは対照的な）データ転送に関連するテレサービス(teleservices)はリモート装置から返送されるアクノリッジ信号(acknowledgement signal)を必要とし、場合によってはさらに専用テレサービスサーバ当てのアクノリッジを必要とする。従って、タイプＢの装置に対しては、アクセス制御がリモート装置からのいくらかの応答を要求するＢ－ＳＡＣに基づくテレサービスのような実施は行えない。伝統的なテレサービスプロトコルはアクノリッジ信号を用いない動作を許可することに寛容ではあるが、システムは依然として、リモート装置が確かに送信されたアクセス制御情報を受信したことの保証を、例えばこの情報を繰り返し再送することによって行わねばならない。この問題はタイプＢの装置が従来の登録手順(registration process)を実行できないという事実によってより大きくなる。すなわち、システムにとってリモート装置の位置を知ることがより困難になり、その結果、リモート装置のお

おまかな位置がわかっている場合と比べて膨大な数の送信局において情報を送信する必要があるであろう。

【００３１】

異なるリモート装置のタイプのいくつかまたはすべてが報知ユーザ情報、例えばＳ－ＢＣＣＨサブチャネル上の証券相場情報を受信することが可能であるという条件を仮定して、いくつかの典型的なＢ－ＳＡＣ実施例を説明する。比較的低レベルなアクセス制御を提供する（しかし、Ａ，Ｂ両タイプのリモート装置に適用可能な）第１の典型的なＢ－ＳＡＣの実施例において、アクセス制御はリモート装置でモニタされる状態変数として提供される。

【００３２】

より具体的には、リモート装置は各同報サービスに関連する状態変数を維持し、この変数はリモート装置が関連する報知サービスを購読しているか否かに応じて有効または無効とされる。状態変数が有効であれば、リモート装置はこの報知サービス、例えば証券相場に関連する情報を表示もしくは出力する。状態変数が無効であれば、リモート装置が情報を読むことが可能であっても、すなわち、この典型的な実施例において情報の暗号化を解くことができるとしても、リモート装置はこのサービスに関連する情報を出力しない。

【００３３】

状態変数はリモート装置のメモリ１８０に維持することができる。メモリ１８０は不揮発性メモリの一部を用いる１つもしくは複数のレジスタか、リモート装置に対応付けされたリムーバブルスマートカードによって構成することができる。いずれの場合も、状態変数は空中インタフェースを介して伝送された特殊メッセージの受信によって有効化もしくは無効化されることが可能である。報知サービスそのものとは異なり、個々のリモート装置が容易に有効化もしくは無効化を行うことができるように、特殊有効化／無効化メッセージはアドレス指定、すなわち装置が特定される。この典型的な実施例によれば、リモート装置の新しいユーザに所定のサービスの無料体験期間を与えるため、リモート装置は１つかそれより多い状態変数が所定の期間、例えば１ヶ月の間、”有効”にプリセットされた状態で製造もしくは販売されてもよい。

【００３４】

状態変数の有効状態は有効かメッセージの受信後所定期間のみ維持することができる。例えば、状態変数有効化信号の受信毎に、保持されていた日付を有効化信号の受信日にリセットすることが可能である。この日付は現在の日付、例えば制御チャネル上で受信、もしくはリモート装置の内蔵時計によって観察された日付と比較を行うこともできる。現在の日付が有効化メッセージの受信からある所定の期間（told）内である限り、有効状態は維持され、リモート装置はこのサービスに関連して報知される情報を出力する。従って、これらの有効化メッセージは購読者が報知サービスから情報を受信し続ける能力に対して命を吹き込むという意味において、"鼓動(heartbeats)"のようなものと見なすことができる。

【００３５】

購読者が購読を中止した場合、システムはその購読者のリモート装置を指定した無効化信号を送信することが可能である。無効化信号は状態変数を無効化された値にリセットし、それによってリモート装置はこのサービスに関連したデータを出力しなくなる。もちろん、無効化信号の受信によって状態変数が有効状態から無効状態へ変化した事実に購読者が気づいた場合、無効化信号がシステムから送られてきそうな期間、例えば購読期間が終了した後、自分の端末の電源を切ることによって購読者がこの無効化処理を妨害しようとするかもしれない。この種の行動の効力は、有効化信号に関する有効期間を用いることによって低下させることができる。本発明による、このＢ－ＳＡＣ技術における典型的な状態変数の使用法は図５に関連して以下に説明する具体例によってより容易に理解されるであろう。

【００３６】

図５において、購読が時刻t_0に活性化(activate)され、タイムライン方向を指す矢印で示されるように、サービスサーバが周期的に有効化メッセージを送信し始める。初めのうちは、これら有効化メッセージは比較的高い頻度で送信される。購読はサービスオペレータによって時刻t_0に活性化されるが、チャネルエラーやリモート装置の電源が切断されているなどの種々の理由のため、リモート装置は時刻t_3まで最初の有効化メッセージを受信できない。従って、リモート

装置はその後、関連する状態変数レジスタに有効化メッセージの受信日／時間をストアし、有効化されたサービスに関連する情報、例えば証券相場情報を図３に示されるＳ－ＢＣＣＨサブチャネル上で受信し始めることが可能になる。以下に説明するように、購読が活性化されている期間、サービスサーバは状態変数レジスタにストアされた受信日／時間をリセットするための有効化信号を周期的に送信する。この受信日／時間は現在の日付＋有効期間と比較されることが可能である。

【００３７】

将来のある時間t_{22}において、購読が中止される。この時点で、又はその少し後で、タイムラインから離れる方向に向かう矢印で示されるように、サービスサーバは無効化メッセージを周期的に送信し始める。これらメッセージの１つをリモート装置が受信すると、このサービスに関連した情報を出力しなくするために、リモート装置は直ちにストアされた状態変数インジケータを無効化する。ある時点で、周波数帯の利用を節約するため、少なくとも１つの無効化メッセージの受信がなされたものと仮定して、サービスサーバはこの特定リモート局宛の無効化メッセージの送信を終了する。

【００３８】

しかしながら、ユーザが所有するリモート装置の電源を、購読が終了する時刻t_{22}よりも前で、無効化メッセージが受信可能となる前の時刻t_{20}において切断した場合を仮定してみる。システムがやがてこの特定リモート装置への無効化信号送信を中止すると仮定すると、他の何らかのアクセス制御機構がない場合、ユーザは無効化信号を受信できない。従って、最後の無効化信号がサービスサーバから送信された、例えば図５の時刻t_{30}の後、ユーザは理論的には再度電源を投入し、報知情報を受信することができる。なぜなら、ユーザ装置の状態変数は依然として有効なままであろうから。典型的な本実施例のこの問題は有効期間t_{old}を用いることによって対処される。

【００３９】

典型的な実施例に従って、状態変数は、無効化メッセージを受信するまで、もしくは最後に受信した有効化信号の日付／時間＋t_{old}が現在の日付／時間を

超えるまでの間だけこのサービスに関する有効状態を維持する。図５に示すように、t_{old}は購読者の装置がその最後の有効化信号（図５において、t_{old}が開始してから２つの連続する”上向き”矢印が示されているように、システムで送信された最後の有効化信号である必要はない）を受信した時点で開始する。t_{old}が時刻t_{45}で終了すると、さらなる有効化信号の受信がないため、状態変数は無効状態にリセットされる。この時点で、証券相場情報はユーザに出力されなくなる。

【００４０】

パラメータt_{old}はリモート装置に予めストアしておいてもよい。その替わりに、エアインタフェースを介してリモート装置に伝送されても良いし、変更可能であっても良い。変更可能な場合、不正を回避するため、t_{old}はある最大時間t_{max}を超えない範囲で変更が許可されるべきである。

【００４１】

本実施例による報知サービスアクセスに関連する周波数帯利用を評価するために、以下の例を考えてみる。

【００４２】

１００万人のユーザがおり、サービスには毎月５万人の新規ユーザが増加し、、５万の購読が毎月中止される場合を仮定する。従って、t_{old}とともに有効化メッセージを受信可能である必要のあるユーザが１００万人いることになる。t_{old}が１ヶ月で、かつこの期間内に各ユーザに対して冗長化を目的として５つの有効化メッセージを送信しなければならないとする。この仮定に基づくと、５００万メッセージ／１ヶ月＝１６６０００メッセージ／日＝７６００メッセージ／時間＝２メッセージ／秒が必要である。上述した典型的なＩＳ－１３６規格準拠のシステムについて、各Ｓ－ＢＣＣＨスロット（０．６４秒毎）に利用可能なペイロードが約１００ビット、各購読者の装置を特定するためのアドレス長が３２ビット、有効化／無効化フラグが１ビットとそれぞれ仮定すると、隠すロット３つの有効化メッセージ又は４．７メッセージ／秒となる。従って、有効化／無効化メッセージはおおよそＳ－ＢＣＣＨスロットの半分の容量を必要とする。オフピーク時間帯において、１つかそれより多いＳ－ＢＣＣＨスロットをこの目

的に割り当てることが可能であるが、ピーク時間帯においては割り当てできない。複数の状態変数に関連する複数のサービスが存在する場合、サービス当たり１ビットのみを追加送信すればよい。しかしながら、サービス識別子(service identifier)はより柔軟なプロトコルを提供することができる。メッセージのフォーマットは、ビット位置及びサービス番号が固定マッピングされた、アドレス、ＳＶ１、ＳＶ２、ＳＶ３という構成であっても、アドレス、ＳＩ１、ＳＶ１、ＳＩ２、ＳＶ２、・・・という構成（ＳＩはサービス識別子）であっても良い。

【００４３】

周波数利用という点に加え、出願人はこの状態変数Ｂ－ＳＡＣ実施例が、今日の業界の慣習において商業的に採算が合うとものであると考える。大部分のユーザがリモート装置内のプログラムを、例えば手動で状態変数をリセットするために、簡単に改竄するだけの十分な技術を持っていないことを鑑みれば、このタイプの不正は商業的なインパクトをサービスプロバイダに与えるとは考えにくい。さらに、これらリモート装置を製造する企業の大きさや、サービス販売ための、またこれら装置の流通経路に対するインセンティブとしてリモート装置に関する価格の報奨金を与えることを考えれば、永久に有効化された状態変数を有する”ブラック”マーケット装置が問題を起こすのに十分な価値があるものとは考えにくい。

【００４４】

状態変数Ｂ－ＳＡＣ実施例は利用の容易性とアクセス制御との有益なバランスをもたらすが、いくつかのサーブビスプロバイダ／システムオペレータはさらなるアクセス制御及び、この種の報知サービスに調和された、あるレベルのデータの完全性を希望するだろう。従って、本発明の別の実施例によれば、サービスプロバイダによって報知される情報は暗号化されてよい。リモート装置は、例えば毎月毎に変更可能な復号（サービス）鍵をダウンロード可能である。ダウンロードのための特別なテレサービスを開発してもよいし、ＥＩＡ／ＴＩＡ　ＩＳ－１３６に示されるＯＴＡテレサービス(Over-the-Air Activation TeleService: ＯＡＴＳ）における追加エレメントであってもよい。復号鍵に加え、有効時間も含まれていて良い。あるいは、キーインデックスが供給される。報知情報サービス

チャネルそれ自身（例えば証券相場）又はＢＣＣＨの汎用位置(general place)において、現在のキーインデックス又は有効時間が供給される。これによって、リモート装置が自らが有するサービス鍵が有効であることを判定することが可能になる。キーインデックス又は有効時間が装置内にストアしたデータと一致しない場合、ユーザは警告を受ける。

【００４５】

本明細書において使用されるサービス鍵という言葉は、強力な算法による暗号化技術を暗示する必要はないことに注意されたい。サービス鍵の最も単純な形式は”ＰＩＮ番号”もしくは、このような状況においてはサービス同定番号（Service Identification Number:ＳＩＮ）であってよい。これはいろいろなサービスから特定のサービスを同定するサービス識別子とは異なる。典型的なユーザにとって容易な何らかの手段を通じてサービス鍵を入力するための用意がなされていない場合、サービス鍵及びキーインデックスは結合することができる。すなわち、ＢＣＣＨ上を明確な形式(clear form)でＳＩＮを送信することができる。しかし、有効期間は提供されることが好ましい。ハッカーはＳＩＮを用意に読むことができるが、通常のユーザがＳＩＮを装置に入力するための簡単な方法はない。

【００４６】

サービス鍵が変更された場合にサービスが中断されるのを防ぐために、システムは前もって、例えば１週間前に、次に用いられるサービス鍵を発行することができる。従って、リモート装置は現在のサービス鍵と次に用いられるサービス鍵の両方を保持することになる。移動局はＢＣＣＨ上で受信する情報に基づいてサービス鍵を自動的に変更する。キーインデックスが用いられる場合には、移動局はサービスの内容を読もうとする前に、まずインデックスをチェックする。日付形式の有効時間が用いられる場合、移動局はＢＣＣＨから日付を探すか、なければ内蔵時計から探すことができる。ユーザが報知サービスを有効にし、装置がサービス鍵が有効でないこともしくは状態変数が無効化されていることを検出した場合（上述したような暗号化がなされていない場合）には、ユーザはディスプレイ及び／又は音による警告を受ける。

【００４７】

サービスプロバイダによって報知されるデータ保護のより単純な形式は暗号化の替わりにスクランブルの単純な形式を用いることである。スクランブルはハッカーによる情報の読み出しを妨害することはできないだろうが、大部分の見込まれる購読者はスクランブルされたデータへアクセスしようとはしないであろう。暗号化に対してスクランブルによってもたらされる利点は計算の複雑さが減少することである。例えば、データもしくはデータの一部分を準秘密変数(semi secret variable)、例えば鍵そのものによって変更することができる。サービスレイヤにおける巡回冗長検査（ＣＲＣ）が変更（例えば鍵との論理的排他和を取る）されても、ＣＲＣの計算においてデータに加えて鍵を含ませても良い。リモート装置がサービス妨害とチャネルエラーとの区別を付けられなくなるため、より低いレイヤのＣＲＣはこの目的で使うべきではない。

【００４８】

図６は本実施例によるスクランブル（又は暗号化）に基づくＢ－ＳＡＣに関連するシグナリングを示す図である。（一番左の、タイムラインへ向かう上向き矢印で示される）最初のイベントはシステムが鍵をk_nにセットする。k_nが依然有効な時刻t_1で、ユーザが報知サービスを要求する。サービスサーバは無線システムを通じてサービス鍵を所定回数送信する。例えば、タイプＢのリモート装置がシステムでサポートされようとしている際、この手順が特に望ましい。この例において、（時刻t_1に続く小さい、タイムラインの方向を示す矢印で示されるように）サービス鍵k_nを含む３度目のメッセージがリモート装置に正しく受信されている。これによりリモート装置が証券相場を報知サービスから読むことが可能な期間が始まる。後の、依然としてk_nが有効な時刻t_{20}において、ユーザがサービスの中止を要求する。システムは何もする必要はないが、その代わりにユーザにサービス鍵の有効期限がなくなるまでサービスの利用を許可することができる。ある所定時刻に於いて、システムは鍵をk_{n+1}に変更する。ユーザはもはやデータの復号を行うことができず、サービスはユーザに提示されることができない。なぜなら、報知情報はいまやこのリモート装置が知らない鍵を用いて暗号化されているからである。図５に関連して上述の実施例で説明した無効化信号とこの暗号化（スクランブル）実施例とを組み合わせ、装置が無効化要求

を受け入れるよう設計されているものと仮定して、システムが無効化信号を装置に送るようにすることが可能であることを当業者は理解するであろう。

【００４９】

図７において、Ｂ－ＳＡＣがスクランブル（または暗号化）によって行われる別の実施例が示されている。図６及び図７の実施例の相違は、図７ではユーザがサービスの中止を要求しないことである。この場合、システムは新しいサービス鍵k_{n+1}を、好ましくは新しい鍵が有効になる前に送信する。装置が少なくとも１つの受信を行う可能性を最大にするため、多くの伝送事例が提供され用いられる。鍵はインデックスもしくは有効時間を有するため、リモート装置は鍵を１つより多く受信した場合、これらが単なる繰り返しであることを知るであろう。k_{n+1}の有効時間が終了するとき、システムは手順を繰り返し、サービス鍵＝k_{n+2}を複数回送信する。この手順はユーザが購読を中止したくなるまで継続され、図６に規定された手順が適用可能になる。

【００５０】

上述の両方の実施例、すなわち状態変数及び暗号化（スクランブル）において、システムは有効化／無効化メッセージまたはサービス鍵のいずれかをリモート装置に送信しなければならない。状態変数メッセージまたはサービス鍵の送信はポイントツーポイントチャネル又は報知チャネル上で行うことができる。図５～７の実施例はアクノリッジされない情報変数又は暗号化（スクランブル）Ｂ－ＳＡＣの実施例という状態で記述されているが、複数のメッセージをリモート装置に送信する”ショットガン”アプローチの他に、これら図面の別の観点を、状態変数又は暗号鍵メッセージがリモート装置によってアクノリッジされる、本発明によるＢ－ＳＡＣ実施例に等しく適用可能であることに注意されたい。

【００５１】

暗号化を用いたＢ－ＳＡＣ実施例のために、サービス鍵は報知チャネルそれ自身によって送信されることが可能である。リモート装置がサービス鍵を読むことができる場合、サービスそのものの情報内容は復号されていることが好ましいので、サービス鍵の伝送についても暗号化されることが好ましい。ここで、サービスはポイントツーマルチポイントサービスであるため、サービス鍵はすべてのユ

ーザに対して同一であることに注意されたい。サービス鍵の伝送を暗号化することによって、詐欺的なユーザはサービス鍵を読むことができなくなり、それを報知サービスからの情報を読むために彼らの装置に使うこともできなくなる。

【００５２】

報知チャネルにおいて、サービス鍵は宛先指定されたメッセージ（すなわち、装置アドレスはメッセージ中に存在する）として配信されることができ、リモート装置に関連するパーソナル（ユニークな）鍵で暗号化される。タイプＡの装置については、サービス鍵を送信する際、従来のセルラ式暗号化技術を適用することができる。すなわち、例えばＯＡＴＳメッセージ又は特殊目的のメッセージの中で送信され、他の音声もしくはメッセージ処理のように（例えば、ＴＩＡ標準のためのＡ鍵に基づいて）暗号化することができる。しかし、サービス鍵の暗号化を特別な（この目的のための）鍵、（ここではＢ鍵と言う）によって実施することも可能である。いかなる情報もその伝送経路で明らかにしないタイプＢの装置については、ＥＳＮもしくは同様の装置識別子をＢ鍵として用いることができる。リモート装置にこのような機能がなければ、タイプＡ及びＢ装置に対して、Ｂ鍵は製造時にロードされるかキーパッドを通じて行われる。タイプＡの装置に対しては、ＯＡＴＳ手順もしくは類似の技術をＢ鍵のダウンロードに用いることができる。タイプＡの装置に対しては、ＭＩＮ／ＩＭＳＩ標準の識別子を、Ｂ鍵メッセージのアドレスとして用いることができる。タイプＢ装置については、そのアドレスは装置識別子（equipment identifier：ＥＳＮ）又は割り当てられたＭＩＮ／ＩＭＳＩであってよい。タイプＡ及びＢの両方のリモート装置について、本明細書では報知識別子番号(Broadcast Identifier Number：ＢＩＮ)と呼ぶ専用の識別子を装置に割り当て、アドレスに用いてもよい。しかし、暗号鍵がはっきりと伝送され、暗号化の目的を失うため、ＥＳＮをＢＩＮ及びＢ鍵の両方には用いないほうがよい。

【００５３】

Ｂ－ＳＡＣの実施例においては、チャネル容量を節約するため、サービス鍵の配信にアクノリッジテレサービス機構(acknowledged teleservice mechanisms)を用いられず、購読の次の期間のためのサービス鍵は送信すべき報知サービスデ

ータが少ないとき、典型的には夜や早朝に送信されうる。従って、ユーザはサービス鍵を交換するためにオフピークの時間帯においてもリモート装置の電源を入れておかねばならない。オフピーク時間帯にリモート装置の電源が投入されたままにされるのは望ましくないが、アクセス制御が増加すること及び暗号化に関連するデータ完全性によってこの問題は相殺されると思われる。

【００５４】

例えば、これらの暗号化（スクランブル）Ｂ－ＳＡＣ実施例は、無資格なユーザがリモート装置のレジスタや信号を操作できる能力を有していたとしても、彼らが報知情報にアクセスすることを妨害する機構を提供する。ユーザがある１つの装置からサービス鍵を読み出せたとしても、他の非購読者が報知情報を読めるようにそのサービス鍵を複数の装置に入力するために必要な知識は非常に専門的なものであり、一般のユーザに容易に提供されるものではない。

【００５５】

例えば正当な復号鍵がない場合又は無効に設定された状態変数を有する場合などによって報知サービスが無効化された場合、特番へ発呼することによってサービスを活性化することが可能であることをユーザが通知されるようにしてもよい。例えば、サービスプロバイダが以下ようなの活性化情報を発行しても良い。活性化情報は課金情報(billing statement)とともに送信されても良い。

【００５６】

【表２】

サービス	月間購読料	購読 (activate)	購読中止 (deactivate)
1.証券相場 （USA Today掲載の全銘柄）	$19.95	*92*23*1	*92*45*1
2.為替相場	$0.95	*92*23*2	*92*45*2
3.オプション	$4.95	*92*23*3	*92*45*3
4.投資信託 （USA Today掲載の全銘柄）	$9.95	*92*23*4	*92*45*4
5.スポーツスコア （全メジャーリーグ。３０分遅れた情報）	$4.95	*92*23*5	*92*45*5

【００５７】

タイプＡのリモート装置では、ユーザは自動音声応答システム(automatic voice prompt system)に転送され、指定されたキーパッド入力の押下による選択の確認を要求される。そして、サービス鍵及び以下に示す他の属性を含むＢ－ＳＡＣテレサービスがダウンロードされる。これらの属性はサービスが有効になったことをユーザに知らせるテキストメッセージを含んでも良い。代わりに、活性化が成功したことを示すために、通常のＳＭＳメッセージがＢ－ＳＡＣテレサービスとともに送信されても良い。ユーザは購読期間を通知されても良い。ユーザが最低購読期間より長い期間を選択した場合、複数のサービス鍵及び関連する属性をダウンロードすることができる。

【００５８】

個人で複数のサービスを購読できるため、個々のサービスはそれぞれの鍵又はサービス状態変数を有する。活性化信号が送信される際、以下の属性が含まれてもよい。サービス識別子、鍵、キーインデックス、有効期間、サービスの変更（予定もしくは最近の変更）、例えば新しいタイプの証券、挨拶文、サービスで問題が発生した場合の電話番号等を説明するテキスト。

【００５９】

システムは移動局の保持内容を確認するため、キーの読み出しを要求しても良い。不正な基地局が移動局の鍵をポーリングするのを避けるため、キーインデックス又は有効日時のみを伝送すれば十分である。これはＬＤＥ通信形式を用いたメンテナンスにも利用可能である。しかし、不正行為を行う基地局から保護を行うための方法は、例えば、通信チャネル又は具体的にはＢ－ＳＡＣテレサービスに強力な暗号化を用いるといったように、他にも存在する。

【００６０】

非活性化が要求されると、オペレータは単に次の復号鍵の送信を行わないか、状態制御技術が用いられている場合には直ちに非活性化信号を送信し、状態を無効化することができる。ユーザが非活性信号の受信を避けようとして電話機の電源を切断する場合、システムは自動的にこのメッセージを再び、例えば装置がレジストレーションを行う際に送信する（通常の移動局、すなわちタイプＡリモート装置の場合）。

【００６１】

タイプＡ２のリモート装置について、サービス鍵等はローカルに入力することができる。これは装置のテストやメンテナンスを行う際に有用であると思われる。例えば、ユーザが自分の所有する装置の動作に関して苦情があり、元の装置を修理に出している間新しい装置を与えられる場合を例として考えてみる。ユーザは自分が購読しているサービスで報知される情報を継続して受信したい。（通常認証用の）Ａ鍵はキーパッドから入力可能であるが、サービス復号鍵は直接入力可能とすべきではなく、より高い安全性を有する形式の暗号化もしくは他の特殊な装置を使用すべきである。さもないと何者かが復号鍵をウエブで公表(publish)することが可能になり、任意のユーザが鍵を自分で入力可能になってしまう。移動電話機内部の保護されたプログラムエリアへのアクセスを行うための安全な手段が開発され、現在用いられている。

【００６２】

Ｂ－ＳＡＣに関連する他の任意の機能を実装することができる。ユーザは購読するサービスのサブセットを受信するために、例えばキーパッドを用いてリモート装置を設定することができる。ユーザは例えば特殊モードに入って、残りの購読期間に関する情報を得ることができる。これは、信用が疑わしいユーザを獲得するための手段として広く用いられるようになってきた従量料金制(pay-per-view)の購読やプリペイドに特に重要であろう。活性化の際、決まった時間のサービスアクセス分の一時払いを受け入れても良い。ユーザは複数の時間枠について購読することが可能であり、従ってある特定のサービスに対するいくつかの鍵をダウンロードすることが可能である。活性化要求が生成される際にユーザがクレジットカード番号を提供することも可能である。スマートカードの用途として、プリペイドサービスの証明書をスマートカードに記憶しても良い。潜在的な複数の時間枠用として、鍵のセット及び属性をカードの製造時にカードへプログラムしておくこともできる。この場合、復号鍵はカードで供給され、装置内での複合化のために装置に送信されても良いし、あるいは復号対象のデータが複合化のためにまずカードに送信され、表示のために装置に送り返すようにしても良い。

【００６３】

要約すれば、タイプBの装置、特にタイプB２の装置を適応させるには、報知チャンネルそのものにおいて状態変数形式の信号もしくは鍵が伝送される、図５に関連する上述の実施例が好ましい。状態変数を用いる方法の利点は装置がそのアドレス以外、システムに知られている他のいかなるパラメータをも必要としないことである。サービスを要求するユーザは、オペレータに（例えば装置に印刷されている）装置のアドレスに関する情報を知らせることができる。しかし、Ｂ鍵は同地に印刷することはできない。従ってサービスオペレータはその後でアドレスと、製造者が装置に入力したＢ鍵との関係を確立する。ＯＡＴＳが利用可能になる前、現在のセルラ式電話において製造者とオペレータの間でＡ鍵を転送するために確立されたものと同一の手順を用いることができる。Ｂ２装置については、Ｂ鍵は変更できない。アドレスとＢ鍵のリンクが失われた場合、装置は動作不可能とされる。Ｂ１タイプのリモート装置については、新しい鍵を入力することによって、アドレス及びＢ鍵との間の新しい関係を確立することが可能である。

【００６４】

オペレータがタイプＡのリモート装置のみ、タイプＢのリモート装置のみもしくはタイプＡ，Ｂの両方のリモート装置のどれをサポートするかを決定すると、ここで説明した原理に従ってＢ－ＳＡＣ手法が開発可能となる。例えば、リモート装置の所在を保全するために、オペレータがＢ－ＳＡＣ設計をタイプＡのリモート装置のみをサポートするものと決定した場合、ほとんどのＢ－ＳＡＣアプリケーションは、状態変数有効化／無効化メッセージもしくはサービス鍵をリモート装置へ送信するために、アクノリッジされた配信テレサービス(acknowledged delivery teleservice)、例えばＯＡＴＳの利用を含むであろう。このような典型的な（暗号化の）実施例は以下の機能のいくつか又は全部を有するであろう。第１に、同報サービス情報の暗号化形式での送信。第２に、（暗号化されたサービス情報の復号に用いられる）サービス鍵の、標準形式を用いた（例えばＡ鍵に基づく）暗号化。第３に、暗号化されたサービス鍵の送信に、例えばＯＡＴＳや専用テレサービスのような、リモート装置からのアクノリッジを必要とする機構を使用すること。第４に、標準のＭＩＮ／ＩＭＳＩを暗号化されたサービス鍵を

含むメッセージのアドレスとして用いること。

【００６５】

これらコンセプトの他のバリエーションもまた可能である。例えば、サービスはさらに、図５に関連して上述した状態変数Ｂ－ＳＡＣ又は図６～７に関連して上述した暗号化Ｂ－ＳＡＣのいずれが用いられているかを示す識別子を送信しても良い。リモート装置は特定のサブチャネル上の報知情報を読むための認証がなされているかどうかを検出するために、その識別子を素早くチェックする。認証がなされていない場合、リモート装置はサービスプロバイダによって与えられた標準メッセージ、例えば”このサービスを活性化するためのさらなる情報を得るには、*888をダイヤルしてください”を出力することができる。

【００６６】

サブチャネル上の同報サービス用の宣伝（または他のタイプの宣伝）もまた、例えば、リモート装置の表示装置上でヘッドラインバナーとして出力することが可能である。例えば、状態変数が無効化されている場合や指定された鍵を持っていない場合など、リモート装置が報知情報を読むための認証を得ていない場合、宣伝が提供されたり、他の報知情報中に宣伝をちりばめてもよい。例えば、有料の報知サービスの内容の説明もしくはそのサブセット（プレビュー(sneak view)）を、報知チャネルそのものによって、又はポイントツーポイントサービスとして提供することができる。報知サービスの説明及び／又はプレビューは宣伝の形式で、より多くの顧客を引きつけるようテイーザーを提供する。

【００６７】

このプレビューの実施例のいくつかの典型的な実施について説明する。なお、これら方法の複数を同時に用いることが可能であることに注意されたい。最初に、アクセス制御を行わずに報知チャネルで宣伝プレビューを提供することができる。サービスの購読申し込みフォームがＢ－ＳＡＣに基づく暗号化もしくはスクランブルを用いて制御されていても、プレビューは暗号化されない。Ｂ－ＳＡＣに関して、関連するチャネルもしくはサブチャネル上で報知される情報のプレビュー部分の独立した識別子、すなわちサービス及びプレビュー部分には暗号化がなされていないことを示す識別子が提供される。この、プレビュー部分のための

識別子の値は、一般に無料サービスのための識別子とは異なっていて良い。従って、ユーザ及び／又は移動局は、有料の報知情報コンテンツのプレビューであることを認識することができる。Ｂ－ＳＡＣに基づく状態変数を用いたアクセス制御を有する類似のプレビュー機構を提供することも可能である。識別子は有料サービスの無料サブセットであることを示す値に設定可能である。有料サービスのためのＢ－ＳＡＣ制御の２つめの実例、すなわち状態変数を有効された状態に設定するほうほうが提供される。一例として、プレビューの内容は、チャネルの有料部分にで利用可能な完全なセットの代わりに、最も売買の少ない株／債券(hold stocks/funds)、最も売買の多い株／債券(active stocks/funds)等でよい。

【００６８】

２つめのバリエーションとして、限られた時間、報知サービス全体をＢ－ＳＡＣの対象から外すことができる。例えば、月に１度、全サービスを無料にすることができる。Ｂ－ＳＡＣに基づく暗号化又はスクランブルが用いられる場合には、暗号化を無効にする。Ｂ－ＳＡＣ制御識別子の値は無料サービス用の値と一般に異なっていて良い。従って、ユーザ及び／又は移動局は有料コンテンツの一時的な無料サービスであることを認識することができる。Ｂ－ＳＡＣに基づく状態変数についても、類似の手法を提供することができる。識別子は無料サービスを示す値に設定することができる。

【００６９】

３つ目のバリエーションとして、例えば報知チャネル又はポイントツーポイントチャネルを用いて、報知情報サービスの実際のサンプルなしで、説明のみを示すメッセージを提供することができる。例えば、証券サービスに対しては、ユーザがＵＳＡ　Ｔｏｄａｙ、ウォールストリートジャーナル又はユーザが理解するであろう他の任意の範囲に掲載される全証券、債券に関する情報が提供されることを説明するメッセージである。スポーツの結果速報チャネルについては、例えばＮＨＬ，ＮＢＡ等、どのリーグのスコアが提供されるのかの範囲をリストすることができる。

【００７０】

ユーザはコマンドを入力することができ、それによってリモート装置は利用可

能な報知サービス及び、どのサービスをユーザが正当に受信可能であるかを表示する（代わりに、ユーザが正当に受信可能なサービスのみをリモート装置が表示しても良い）。あるオペレータでは有料で、他のオペレータでは無料で利用可能な特定のサービスが存在しても良い。ユーザはより詳細な情報を得るためにメニューから表示されたサービスを選択することができる。このようにして、リモート装置は報知サービスに関する説明をユーザに提示する。

【００７１】

プレビューそれ自身に関する情報、一時的に無料なコンテンツであること及びプレビューコンテンツの説明は、リモート装置又はユーザに、例えば以下のようにして提供することが可能である。

（１）例えば、プレビューチャネルがあること、いつ全チャネルが無料なのか、説明チャネル、お試しチャネル及び無料チャネルはどこでどのようにして（例えばどのキーパッド入力を使うか）見つけられるのかといった宣伝を、料金情報の中に宣伝を含ませる。

（２）無線システム、例えばＳＭＳメッセージを用いて、又はファクシミリを用いてユーザに情報を送信する。

（３）例えば、サービスオペレータのウエブサイトにおいて、報知チャネルの情報のシミュレート（例えば最新のデータでない）バージョンもしくは、現在無線チャネルで送信されているものの複製（ただし、２つの送信手段の間には、所定の実装及びプロトコルの制限により見込まれる遅延がある）を表示する。ユーザは、購読した場合、無線サービス及びユーザ装置とのインタフェースとして、どのようにサービスが見えるのかに関する実際的な表示を提供するために更新されるコンテンツとともに、ラップトップもしくは他の装置を表す、シミュレートされた画面を見るであろう。

【００７２】

プレビューを示す識別子提供の代替え方法として、プレビューを得るための復号鍵をすべての移動局、又はシステムもしくはサービスオペレータに選択された移動局に送信する方法がある。チャネルの、プレビュー部分と及び他の部分は異なる鍵によって暗号化される。この例に関する問題は、定期購読者が必ず２つの

サービス鍵を持つ必要があること、又はプレビューコンテンツが通常のサービスの中で繰り返される必要があること、プレビューのみのユーザに対しても暗号化技を与えなければならず、鍵の配信要求が増加することである。同様の方法を（及び結果として得られる問題点をも）Ｂ－ＳＡＣに基づく状態変数を用いた報知サービス及び、（プレビューと対立するものとしての）無料チャネルに適用することができる。

【００７３】

多種のマーケットの要望にサービスを適合させるために、異なる属性を有する特別な報知サービスが配信及び／又は販売されても良い。例えば、証券相場サービスがリアルタイムに、又はある時間遅れて配信されて良い。無線インタフェースを介してサービスを配信するためにはいくらかの時間がかかるため、ここでは"リアルタイム"な報知情報サービスをリアルタイムに近い(Near Real Time：ＮＲＴ)サービスと表記する。すなわち、サービスサーバでは情報はリアルタイムだが、チャネルエラーを含む配信時間によって、情報をエンドユーザに配信するのにはいくらか余計に時間がかかる。従って、リアルタイムサービスとして販売することはできない。その代わり、ユーザはより安い料金で遅れたサービスを購読することができる。２つの論理サブチャネル（又は論理サブチャネルのセット）を、同一の報知情報に関連するＮＲＴサービス及び遅れのあるサービスの両方の目的のために割り当てることが可能である。別個の状態変数又は復号鍵がそれぞれに用いられる。しかし、この並行サービス伝送は必要とする周波数帯域を、高速及び低速サービスの両方の和まで増加させる。別の、より効率的な解決方法はＮＲＴサービスのみを伝送することである。

【００７４】

Ｂ－ＳＡＣ方式が状態変数のコンセプトに基づいて報知サービスに実装された場合、個々のサービスレベルは自身のサービス識別子（ＳＩ）を有する。ＮＲＴサービスを提供するため、ＳＩの１つは、到着したデータを全くの制限なしで表示することをリモート装置に許可する。第２のＳＩは、遅れのあるサービスを提供するため、装置の設計によって報知情報の表示を所定の時間だけ遅らせることを暗示する。いずれのＳＩもＢＣＣＨ上で送信される。代わりに、共通のＳＩと

、遅れのある表示を示すための、ＳＶが更新された際に装置に送信される他の識別子を用いても良い。必要とされる遅延は、サービスそのものに付随して、例えばＢＣＣＨ上で送信されることができる。その代わりに、遅延を製造者によって入力することや、ポイントツーポイントサービスとして無線リンクを介して送信するようにしても良い。

【００７５】

Ｂ－ＳＡＣ方式が暗号化のコンセプトに基づいて実装された場合、両者のサービスレベルは同一時刻に読み出され、従って共通の鍵を用いる。鍵の配信時に、リモート装置がデータ表示前に遅延を挿入すべきか否かを通知するさらなる識別子が装置に送信される。別の、サービスを不正利用からより強力に保護する方法は、サービスデータとともに秘密変数(secret variable)を供給することである。この変数は非ＮＲＴ購読者に対して予測不可能な方法で周期的に変化する。従って、基本的な暗号化に加え、報知情報サービスコンテンツ全体がこの秘密変数によってスクランブルもしくは暗号化される。この秘密変数は要求された遅延が発生した時点で、暗号化されずに、又は基本となる暗号化の保護の元に送信することが可能である。非ＮＲＴ購読者はこの変数がチャネル上に存在し、サービスデータを完全に復号可能となるまで待たねばならない。変数が最後に存在した時点から受信した以前のサービスデータは変数及び基本となる復号鍵を用いて復号される。秘密変数はおおよそ規定された遅延が発生した時点で、チャネルエラーの影響を減少させるために繰り返し送信することができる。ＮＲＴ購読をしているリモート装置は、キー配信とともにデータを全くの遅延なしで復号可能であるような情報を受信する。例えば、秘密変数の出力に非線形シフトレジスタを用いることができる。所定時刻t_{i_c}（t_{i_c}は遅延に関してインクリメントされる）におけるこのシフトレジスタの内容を装置は知っており、従って秘密変数の現在値を計算して到着するサービスデータを復号することができる。

【００７６】

リモート装置内でハードコードによらない遅延を有することによって、オペレータが遅延を変更することが可能になる。遅延は装置固有であるため、２レベルより多いレベル数の遅延を用いることも可能であるし、またＢＣＣＨによって複

数の遅延を伝送することも可能である。遅延配信に関する見解は、時間／コストが変化しやすいと考えられる任意の報知サービス情報、例えばスポーツ結果などに適用することができる。

【００７７】

ＮＲＴが、例えば、市場のインデックス、もっとも激しく取り引きされた(heavily treaded)銘柄、もっとも共通に保有された(commonly held)銘柄等、遅延されたサービスによって提供される情報の概要のみを提供するようにサービスを構成することもできる。この概要は遅延されたサービスにおいても同様に提供されても、されなくてもよく、すなわち概要は遅延されるサービスのサブセットであってもよい。この構成は、サービス範囲全体ではＮＲＴにおいて送信可能な周波数帯の容量より多い容量が必要な場合に注目されるであろう。すなわちサービスに関連してより高速な情報が配信されようとしているので、より短い周期及び高速な周波数帯が必要とされる。もしＮＲＴモードにある特定のサービスのための報知情報のすべてを供給することが実行できそうもない場合には、サービスをＮＲＴモードでは要約、完全版を遅延されたモードとして構成することによって、サービスプロバイダが継続して複数レベルのサービスを販売可能であるような方法を提供する。従って、ユーザはＮＲＴ要約サービスだけ、内容の多い、遅延されたサービスだけ、もしくは両方を購読することができる。さらに、適切な数の鍵又はＳＩ／ＳＶが購読中のリモート装置へ配信される。

【００７８】

異なるレベルのサービスをうまく表現することに加え、リモート装置は報知情報サービスをそれら装置の消費電力を節減するような方法で読むように動作することができる。従って、有効な鍵もしくは有効な状態の状態変数を有することによってリモート装置がアクセスした報知サービス情報を常に読んでいるわけではない。例えば、ユーザは自らのリモート装置を特定の購読サービスを１時間に１ど、もしくは１０分ごとに読むように設定することができる。異なるサービスレベル又は異なる部分（例えば上述した証券相場サービスの異なるサブチャネル）に対して、リモート装置の読み込み周期性はサービスレベル又はサービス部分によって変化してもよい。典型的なサービス部分はまた、特定のポートフォリオの

一部である、複数の株インデックスまたは証券を含む。さらに、読み出しは単純に所定時間間隔ではなく、よりインテリジェントな機構によって起動されてもよい。上述した、要約ＮＲＴ及び内容のより多い遅延されたサービスを用い、ユーザは自らのリモート装置を、要約ＮＲＴを各周期または周期的（例えば１０分）毎に、読むよう設定することができる。その後、興味のある特定の証券／インデックスに関する情報を要約ＮＲＴで読んだら、リモート装置はユーザによってより情報の多い、遅延されたサービスを読むようにユーザによって設定されうる。かわりに、より情報の多い、遅延されたバージョンのサービスを自動的に読む替わりに、あらかじめ設定されたユーザトリガ条件の発生を認識すると、リモート装置にユーザへ、より情報の多い、遅延されたサービスを読むべきかどうかのクエリを出力する。ユーザはリモート装置に、例えば所望の情報の１周期を読むように要求することができる。この要求は例えば所定の読み出し時間に基づく周期のサブセットや、全周期を読もうとする試みに限定されることも可能であるが、ビットエラーが発生した場合には、所定の読み出し総時間、全周期における情報の最低割合等に限定される。情報が利用可能である場合には、ユーザが変更されるか又はアイコンがリモート装置の画面に表示される。

【００７９】

もちろん、リモート装置が報知情報サービスからの新しい情報を取得したからといって、直ちにユーザへの表示が整えられる訳ではない。従って、リモート装置はユーザが選択可能ないくつかの情報表示オプションを有することが可能である。あるモードにおいては、情報は取得された状態で自動的に表示される。別のモードにおいては、新しい情報が取得されたら、装置がアイコン等、聴覚又は視覚に訴える提示を行い、新しく取得した情報を出力する前にいくらかの追加入力をユーザに要求する。

【００８０】

上述し、本明細書に参照として組み入れられる米国特許出願、「無線通信システムを介して送信される情報サービスのためのチャネル化及びエンコード技術(Channelization and Encoding Techniques for Information Services Transmitted Via Radiocommunication Systems)」において述べられるように、報知情報サ

ービスによって提供される情報は、報知（すなわちポイントツーマルチポイント）リソース及び／又は非報知（すなわちパケットデータを含むポイントツーポイント）リソースを用い、システムによって伝送可能である。例えば、移動局がインターネットを介してアクセス可能なサーバからのダウンロードを経由して、企業名及び株シンボル（又は単なる番号）との間の関連、すなわち図３の実施例において証券名サブチャネルで見つかる情報のタイプを、アドレス指定されたメッセージによって受信した場合を考えてみる。その場合、システムは開始値サブチャネル及びデルタサブチャネルを報知するだけでよい。替わりに、開始値サブチャネル上でみつかる情報もまた、アドレス指定されたメッセージを用いてリモート装置に供給することができる。

【００８１】

３つの全サブチャネルがアドレス指定されたメッセージとして提供されたとする。例えば、リモート装置が一旦証券名及び開始値サブチャネルに関連する情報をダウンロードすると、リモート装置はＳＭＳを介してデルタチャネル情報、例えば特定の株シンボル又は番号を要求することが可能になる。別の方法としては、ユーザにサービスサーバを用いてポートフォリオを定義可能とする方法もある。そして、リモート装置は全体のポートフォリオに関する情報を単に問い合わせる要求を開始する。この要求に応答して、サービスサーバは、開始値及びデルタチャネルの両方もしくは単にデルタチャネルに関する情報を含んだこの情報をテレサービスを介して提供することができる。他の可能性としては、この情報をダウンロードさせるあらかじめ定義されたトリガである。

【００８２】

本発明を証券相場サービスに関して説明してきたが、本発明が、他の、ユーザに情報が報知されるようなシステムに対して同様に適用可能であることを当業者は理解するであろう。

【００８３】

さらに、ここで説明されたＬＤＥはケーブル、赤外線装置、キーパッド又は無線短距離通信リンクであってよい。ＬＤＥはＰＣ又は、オペレータ又はディーラによって所有、操作される特殊プログラミングユニットと通信可能である（ユー

ザは復号鍵を電子メール及び装置と通信するプログラムとして入手してもよい）。上述の説明により教授された技術の多くの変形及び組み合わせは以下の請求範囲に記述される本発明の精神又は範囲を超えることなく当業者によって発明されうる。

【図面の簡単な説明】

【図１】

本発明に利用可能なハイパーフレームの構成を説明する図である。

【図２】

本発明に利用可能なＤＣＣＨの論理チャネルを説明する図である。

【図３】

本発明によるセキュアな相場サービスに関連する報知情報に用いられる論理チャネルの典型的な再分割(subdivision) 例を示す図である。

【図４】

本発明を適用可能な典型的な無線電話システムを示す図である。

【図５】

本発明の典型的なステータス変数の実施例を説明するのに用いられる信号タイムラインを示す図である。

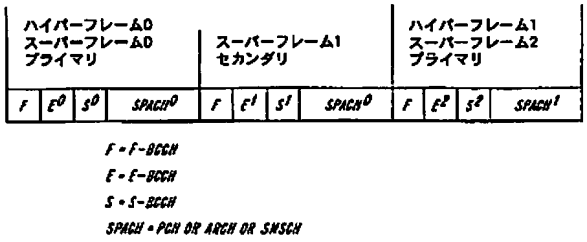
【図６】

本発明の典型的な暗号化（スクランブル）の例を説明するのに用いられる信号タイムラインを示す図である。

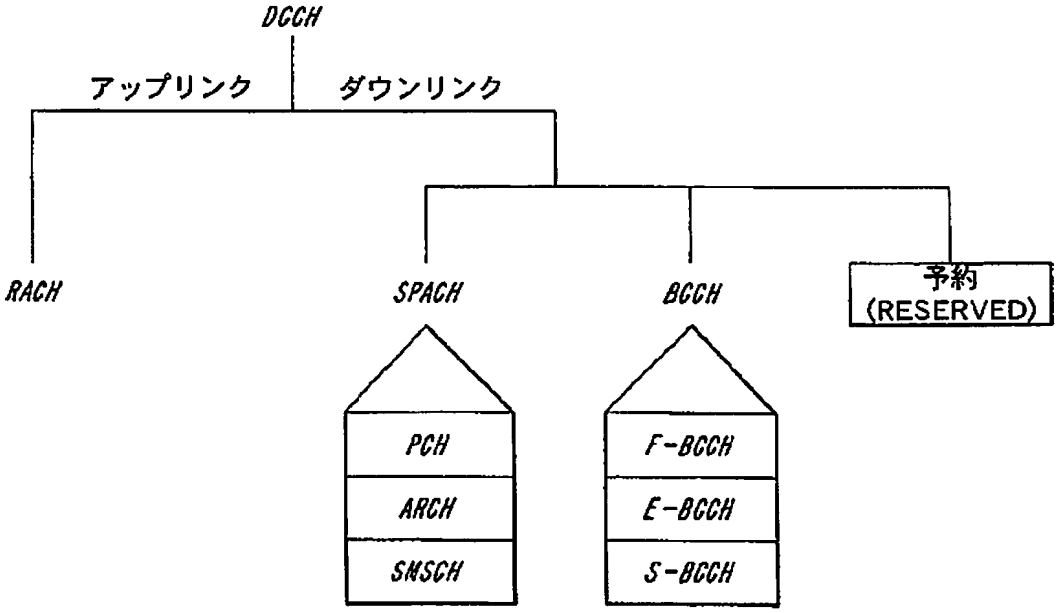
【図７】

本発明の典型的な暗号化（スクランブル）の例を説明するのに用いられる信号タイムラインを示す図である。

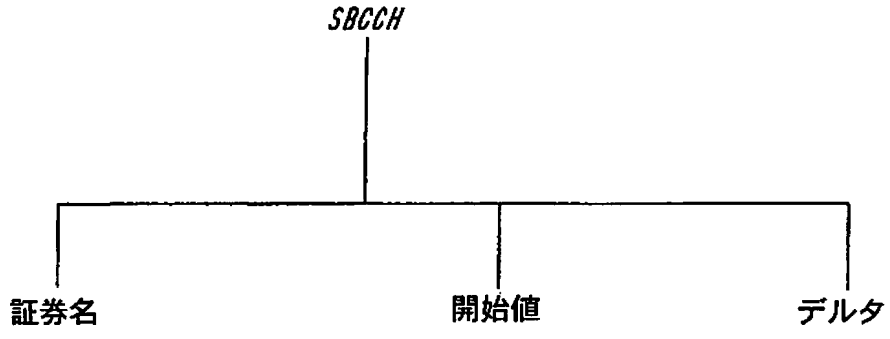
【図１】


ハイパーフレーム0
スーパーフレーム0
プライマリ
スーパーフレーム1
セカンダリ
ハイパーフレーム1
スーパーフレーム2
プライマリ
F
E0
S0
SPACH0
F
E1
S1
SPACH0
F
E2
S2
SPACH1
F = F-BCCH
E = E-BCCH
S = S-BCCH
SPACH = PCH OR ARCH OR SMSCH

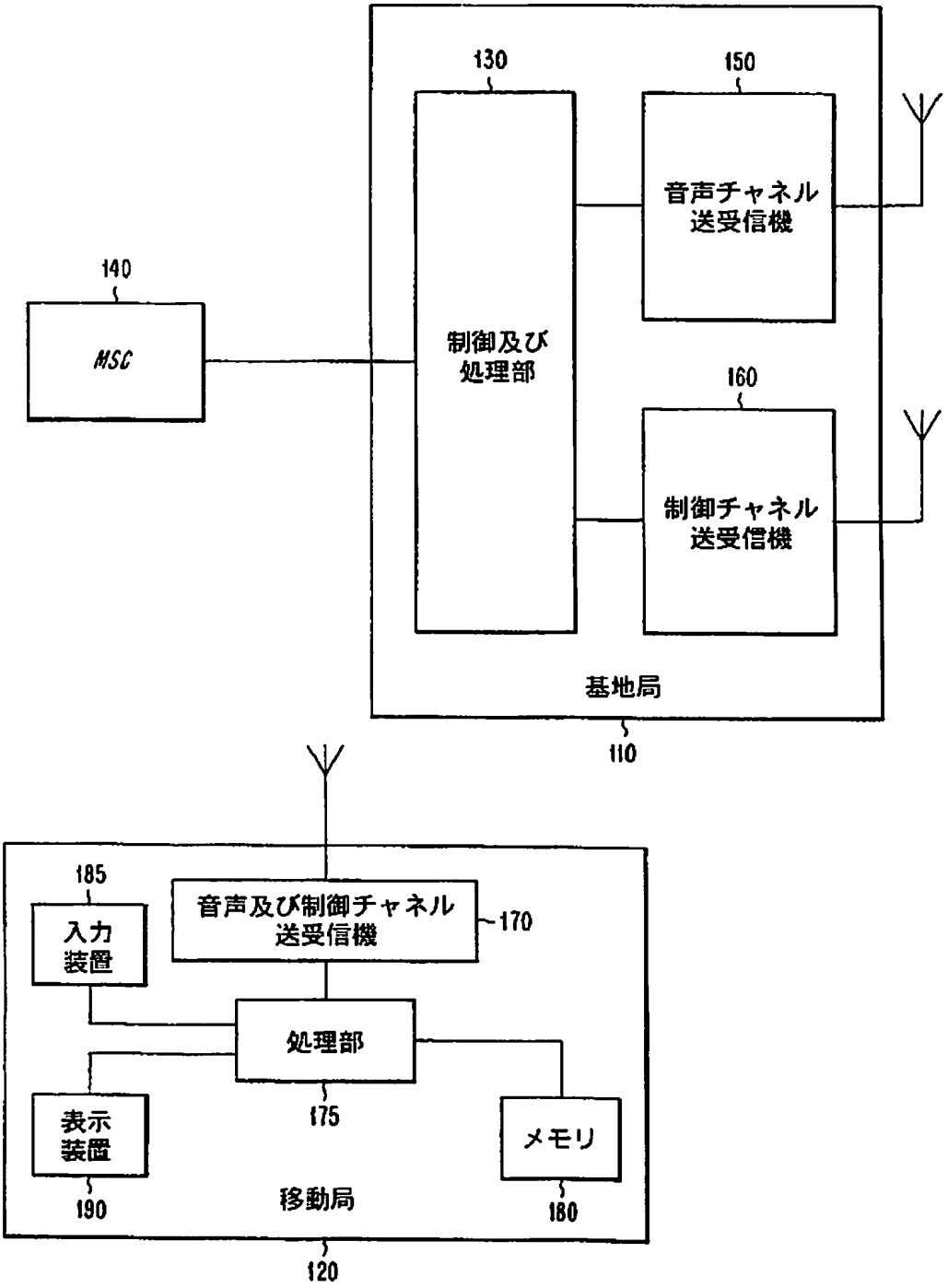
【図２】


DCCH
アップリンク
ダウンリンク
RACH
SPACH
BCCH
予約
(RESERVED)
PCH
ARCH
SMSCH
F-BCCH
E-BCCH
S-BCCH

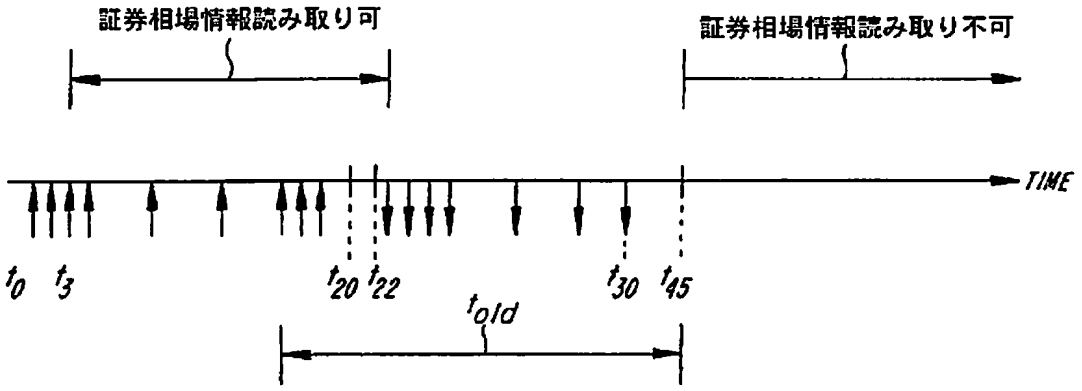
【図３】


SBCCH
証券名
開始値
デルタ

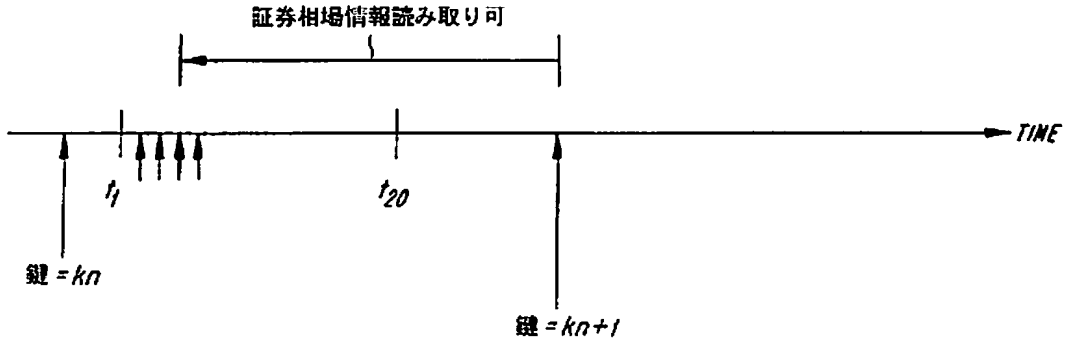
【図４】


130
150
音声チャネル
送受信機
140
MSC
制御及び
処理部
160
制御チャネル
送受信機
基地局
110
185
入力
装置
音声及び制御チャネル
送受信機
170
処理部
175
表示
装置
190
メモリ
180
移動局
120

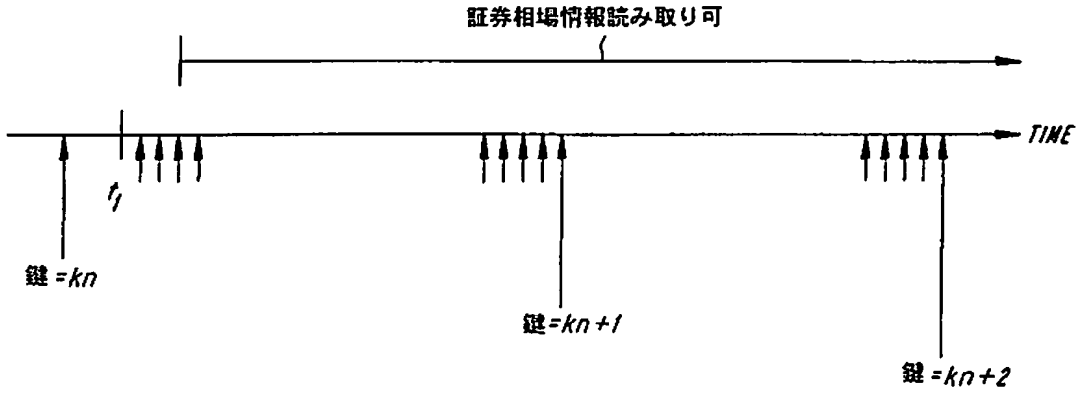
【図５】


証券相場情報読み取り可
証券相場情報読み取り不可
TIME
t_0 t_3 t_{20} t_{22} t_{30} t_{45}
t_{old}

【図６】


証券相場情報読み取り可
TIME
t_1
t_{20}
鍵＝kn
鍵＝kn+1

【図７】


証券相場情報読み取り可
TIME
t_1
鍵＝kn
鍵＝kn+1
鍵＝kn+2

【手続補正書】特許協力条約第３４条補正の翻訳文提出書
【提出日】平成１２年６月１６日（２０００．６．１６）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】　無線通信システムにおける報知情報サービスに対するアクセスを制御する方法であって、
前記報知情報サービスに関連する情報を暗号化するステップと、
前記システムによって、前記暗号化された、複数のリモートユニットによって利用可能な情報をエア・インタフェースを介して報知するステップと、
前記暗号化された情報を、前記複数のリモート局のうちの購読中の１つへアドレス指定されたメッセージの一部として復号するために利用可能なサービス鍵を前記システムによって伝送するステップ、及び、
前記サービス鍵を周期的に変化させるステップとを有することを特徴とする方法。
【請求項２】　前記サービス鍵を前記システムによる伝送前に暗号化するステップをさらに有することを特徴とする請求項１記載の方法。
【請求項３】　前記サービス鍵を暗号化するステップが、
前記サービス鍵をＡ鍵手法を用いて暗号化するステップをさらに有することを特徴とする請求項２記載の方法。
【請求項４】　前記サービス鍵の受信を、前記複数のリモート局のうちの購読中の１つによってアクノリッジするステップをさらに有することを特徴とする請求項１記載の方法。
【請求項５】　前記サービス鍵を伝送するステップが、
前記サービス鍵の伝送にＯＡＴＳ(Over-the-air Activation TeleService)を用いるステップをさらに含むことを特徴とする請求項４記載の方法。

【請求項６】　前記サービス鍵を伝送するステップが、

前記サービス鍵を報知チャネルで伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項７】　前記サービス鍵を伝送するステップが、

前記サービス鍵をポイントツーポイントチャネルで伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項８】　さらに、

前記変更されたサービス鍵を用いて前記情報を暗号化する前に、所定時間前記変更されたサービス鍵を前記複数のリモート局のうち現在購読中のリモート局に対して伝送するステップを有することを特徴とする請求項１記載の方法。

【請求項９】　前記情報を暗号化するステップが、前記情報を所定の変数を用いてスクランブルするステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１０】　前記サービス鍵を伝送するステップが、

前記サービス鍵とともに、前記サービス鍵が前記情報の復号化に利用可能な有効期間を伝送することを特徴とする請求項１記載の方法。

【請求項１１】　前記サービス鍵を伝送するステップが、

前記サービス鍵とともに、リモート装置が前記サービス鍵が有効であるかどうかを判断するのに利用可能なキーインデックスを伝送する方法。

【請求項１２】　前記サービス鍵を伝送するステップが、

個人識別番号（ＰＩＮ）及びサービス識別番号（ＳＩＮ）の１つを前記サービス鍵として供給するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１３】　さらに、

前記複数のリモート局のうちの前記現在購読中の１つにおいて、前記変更されたサービス鍵及び前記サービス鍵を保存するステップ及び、

前記システムによって１回に報知された前記情報の復号に前記変更されたサービス鍵を用いるステップを有することを特徴とする請求項８記載の方法。

【請求項１４】　前記サービス鍵を伝送するステップが、

前記サービス鍵を周期的な間隔で繰り返し伝送するステップをさらに有することを特徴とする請求項１記載の方法。

【請求項１５】　無線通信システムにおける報知情報サービスに対するアクセスを制御する方法であって、

前記報知情報サービスに関連する情報であって、複数のリモートユニットが利用可能な情報を、前記システムによってエア・インタフェースを介して伝送するステップと、

有効化信号を、前記複数のリモート局のうち購読中のリモート局宛のメッセージの一部として、前記システムによって伝送するステップ、及び、

前記複数のリモートユニットの１つが自分に宛てられた有効化信号を受信した場合、前記複数のリモートユニットの１つにおいて前記情報を出力するステップとを有することを特徴とする方法。

【請求項１６】　前記複数のリモート局のうち購読中のリモート局によって、前記有効化信号の受信をアクノリッジするステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１７】　前記有効化信号を伝送する前記ステップが、

前記有効化信号を報知チャネルで伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１８】　前記有効化信号を伝送する前記ステップが、

前記有効化信号をポイントツーポイントチャネルで伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項１９】　前記有効化信号を伝送する前記ステップが、

前記有効化信号を周期的な感覚で繰り返し再伝送するステップをさらに有することを特徴とする請求項１５記載の方法。

【請求項２０】　少なくとも１つの報知リソースにおいて報知情報サービスに関連する報知情報を受信するとともに、前記報知情報サービスに関連する有効化及び無効化メッセージを受信する受信機と、

前記有効化及び無効化メッセージの受信に基づいて値が変化する、有効化／無効化状態変数を保持するメモリ装置、及び、

前記有効化／無効化状態変数が有効化の値を有する場合のみ前記報知情報を出力する出力装置とを有することを特徴とする移動局。

【請求項２１】　前記購読中のリモート局が前記暗号化情報へのアクセスを得るための料金を負うことを特徴とする請求項１記載の方法。

【請求項２２】　前記料金が銀行口座又は前払い口座から控除されることを特徴とする請求項２１記載の方法。

【請求項２３】　前記料金がクレジット口座につけられることを特徴とする請求項２１記載の方法。

【請求項２４】　少なくとも１つの報知リソースにおいて報知情報サービスに関連する暗号化された報知情報を受信するとともに、前記暗号化された情報を復号するために利用可能なサービス鍵を受信する受信機と、

前記サービス鍵を保持するメモリ装置、及び、

前記暗号化情報が前記サービス鍵によって復号され次第前記報知情報を出力する出力装置とを有することを特徴とする移動局。

【請求項２５】　前記サービス鍵が前記報知情報サービスによって伝送される前に暗号化されていることを特徴とする請求項２４記載の移動局。

【請求項２６】　前記サービス鍵がＡ鍵手法に従って暗号化されていることを特徴とする請求項２５記載の移動局。

【請求項２７】　前記サービス鍵が予め定められた期間有効であることを特徴とする請求項２４記載の移動局。

【請求項２８】　前記受信機が予め定められた期間の満了前に、次のサービス鍵を受信することを特徴とする請求項２７記載の移動局。

【請求項２９】　報知情報サービスを当該報知情報サービスの購読者に提供する無線通信システムであって、

前記報知情報を暗号化する暗号化手段と、

前記暗号化された報知情報及び前記暗号化された報知情報の復号に使用可能な鍵を伝送する伝送手段、及び、

前記暗号化された報知情報及び前記伝送された鍵を受信する、少なくとも１つのリモート受信手段とを有し、

さらに前記受信手段が、

前記鍵を前記暗号化された情報の復号に用いるプロセッサ手段と、

前記復号された情報が受信されてから予め定められた時間後に前記復号された情報を出力する出力手段とを有することを特徴とする無線通信システム。

【請求項３０】　前記情報が金融市場動向を含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３１】　前記情報がスポーツのスコアを含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３２】　前記情報がニュースの見出しを含むことを特徴とする請求項２９記載の無線通信システム。

【請求項３３】　無線通信システムにおける報知情報サービスへのアクセスを提供する方法であって、　前記報知情報サービスに関連する情報の部分を暗号化するステップと、　前記システムによって、前記報知情報サービスに関連する情報であって、複数のリモートユニットに利用可能な情報を、エア・インタフェースを介して報知するステップと、　前記システムによって、前記情報の暗号化された部分を復号するのに使用可能なサービス鍵を、前記複数のリモート局のうちの、選択されたリモート局宛てメッセージの一部として伝送するステップ、及び、　前記サービス鍵を周期的に変更するステップとを有することを特徴とする方法。

【請求項３４】　前記鍵が前記リモート局のうち購読中のリモート局に伝送されることを特徴とする請求項３３記載の方法。

【請求項３５】　前記報知情報が前記報知情報サービスのための宣伝メッセージを含み、前記メッセージが前記リモート局のうち、購読中でないリモート局へ送信されることを特徴とする請求項３３記載の方法。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inter ional Application No
PCT/SE 99/00929

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L9/08 H04H1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L H04Q H04H H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 708 960 A (KAMISAKA TADAYUKI ET AL) 13 January 1998 (1998-01-13)	1,6,7, 15,17, 18,29-35
A	abstract column 1, line 35 -column 2, line 32 column 12, line 58 -column 13, line 28 figures 1,2	8,14,19

A	US 5 117 458 A (TAKARAGI KAZUO ET AL) 26 May 1992 (1992-05-26)	1,15,20, 21,24, 29,34
	abstract column 3, line 50 -column 4, line 36 figures 2,7,10,20	

	-/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 October 1999	20/10/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Gautier, L

Form PCT/ISA/210 (second sheet) (July 1992)

page 1 of 2

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/SE 99/00929

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 132 401 A (TOKYO SHIBAURA ELECTRIC CO) 30 January 1985 (1985-01-30) abstract page 4, line 5 -page 7, line 9 figures 1,4	1,14,15, 19,24, 29,31,34
P,X	EP 0 915 580 A (GLOBALSTAR LP) 12 May 1999 (1999-05-12) abstract page 2, line 3 - line 43 page 3, line 15 - line 42 page 7, line 34 -page 8, line 37 claim 1 figures 1,18,2	1,2,4-7, 9,15-21, 24,25, 29-36

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/SE 99/00929

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5708960	A	13-01-1998	JP	7231309 A	29-08-1995
			GB	2286751 A,B	23-08-1995
US 5117458	A	26-05-1992	JP	4038029 A	07-02-1992
			JP	2821204 B	05-11-1998
			JP	3145835 A	21-06-1991
EP 0132401	A	30-01-1985	JP	60183842 A	19-09-1985
			JP	60024792 A	07-02-1985
			CA	1219930 A	31-03-1987
EP 0915580	A	12-05-1999	JP	11205303 A	30-07-1999
			WO	9923827 A	14-05-1999

Form PCT/ISA/210 (patent family annex) (July 1992)

フロントページの続き

(31)優先権主張番号　０９／１３２，２３２
(32)優先日　　平成10年８月11日(1998. 8. 11)
(33)優先権主張国　米国（ＵＳ）
(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＣＹ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＧＷ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＧＨ，ＧＭ，ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＬ，ＳＺ，ＵＧ，ＺＷ)，ＥＡ(ＡＭ，ＡＺ，ＢＹ，ＫＧ，ＫＺ，ＭＤ，ＲＵ，ＴＪ，ＴＭ)，ＡＥ，ＡＬ，ＡＭ，ＡＴ，ＡＵ，ＡＺ，ＢＡ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＵ，ＣＺ，ＤＥ，ＤＫ，ＥＥ，ＥＳ，ＦＩ，ＧＢ，ＧＤ，ＧＥ，ＧＨ，ＧＭ，ＨＲ，ＨＵ，ＩＤ，ＩＬ，ＩＮ，ＩＳ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＣ，ＬＫ，ＬＲ，ＬＳ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＫ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＧ，ＳＩ，ＳＫ，ＳＬ，ＴＪ，ＴＭ，ＴＲ，ＴＴ，ＵＡ，ＵＧ，ＵＺ，ＶＮ，ＹＵ，ＺＡ，ＺＷ